

[Previous Doc](#) [Next Doc](#) [Go to Doc#](#)
[First Hit](#)

☐ **Generate Collection**

L1: Entry 7 of 7

File: JPAB

Oct 26, 2001

PUB-NO: JP02001298779A
DOCUMENT-IDENTIFIER: JP 2001298779 A
TITLE: MOBILE INFORMATION TERMINAL AND SERVICE SYSTEM USING IT

PUBN-DATE: October 26, 2001

INVENTOR-INFORMATION:

NAME

TAKAHASHI, KIYOSHI

COUNTRY

ASSIGNEE-INFORMATION:

NAME

MITSUBISHI ELECTRIC CORP

COUNTRY

APPL-NO: JP2000113594

APPL-DATE: April 14, 2000

INT-CL (IPC): H04Q 7/38; G09C 1/00; H04L 9/32; H04M 1/67; H04M 3/00; H04M 3/42;
H04M 11/00

ABSTRACT:

PROBLEM TO BE SOLVED: To provide a mobile information terminal that can receive services after authentication of a user once and to provide a service system using it.

A

SOLUTION: The service system is provided with a data processing unit that collates fingerprint data and a terminal identification code sent from the mobile information terminal with fingerprint data-terminal identification code information that cross-references fingerprint data of a person registered as a user of the mobile information terminal and a terminal identification code identifying the mobile information terminal and issues an authentication code with a validity on the basis of the result of collation, the mobile information terminal that reads the fingerprint, generates the fingerprint data, transmits the fingerprint data and the terminal identification code stored in advance to the data processing print and stores the received authentication code and the validity, and a service terminal that receives the authentication code. The service system provides services to the user of the mobile information terminal on the basis of the authentication code received by the service terminal.

COPYRIGHT: (C) 2001, JPO

[Previous Doc](#) [Next Doc](#) [Go to Doc#](#)

CP
B
MD
A
C

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-298779

(P2001-298779A)

(43) 公開日 平成13年10月26日 (2001. 10. 26)

(51) IntCl. ⁷	識別記号	F I	テーマコード* (参考)
H 0 4 Q 7/38		G 0 9 C 1/00	6 6 0 E 5 J 1 0 4
G 0 9 C 1/00	6 6 0	H 0 4 M 1/67	5 K 0 2 4
H 0 4 L 9/32		3/00	B 5 K 0 2 7
H 0 4 M 1/67		3/42	Z 5 K 0 5 1
3/00		11/00	3 0 2 5 K 0 6 7

審査請求 未請求 請求項の数12 O L (全 14 頁) 最終頁に続く

(21) 出願番号 特願2000-113594(P2000-113594)

(22) 出願日 平成12年4月14日 (2000. 4. 14)

(71) 出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72) 発明者 高橋 清

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(74) 代理人 100102439

弁理士 宮田 金雄 (外1名)

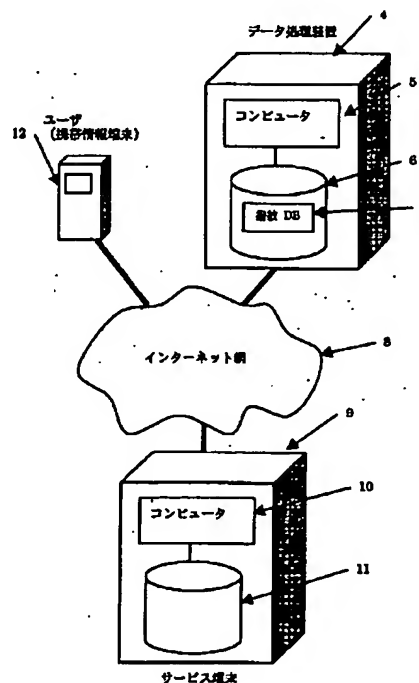
最終頁に続く

(54) 【発明の名称】 携帯情報端末およびこれを用いたサービスシステム

(57) 【要約】

【課題】 一度の本人認証を行うことにより、複数のサービスの提供を受けることができる携帯情報端末とこれを用いたサービスシステムを提供する。

【解決手段】 携帯情報端末の使用者として登録された者の指紋データと携帯情報端末を識別する端末識別符号とを対応させた指紋データ-端末識別符号情報に、携帯情報端末から送信された指紋データと端末識別符号を照合し、この照合結果に基づき有効期限を付けた認証符号を発行するデータ処理装置と、指紋を読み取り指紋データを生成し、指紋データとあらかじめ記憶された端末識別符号をデータ処理装置へ送信し、受信した認証符号と有効期限を記憶する携帯情報端末と、認証符号を受信するサービス端末とを含み、サービス端末で受信された認証符号に基づいて携帯情報端末の使用者へサービスが提供されるサービスシステム。



【特許請求の範囲】

【請求項1】 携帯情報端末の使用者として登録された者の指紋データと前記携帯情報端末を識別する端末識別符号とを対応させた指紋データ-端末識別符号情報に、前記携帯情報端末から送信された指紋データと端末識別符号を照合し、この照合結果に基づき有効期限を付けた認証符号を発行するデータ処理装置と通信を行うものであって、指紋を読み取り指紋データを生成する指紋読み取り手段、前記指紋データと、あらかじめ記憶された前記端末識別符号とを前記データ処理装置へ送信する送信部、前記データ処理装置において発行された認証符号を受信する受信部、およびこの受信部で受信された前記認証符号と有効期限をあわせて記憶する記憶部を備えたことを特徴とする携帯情報端末。

【請求項2】 送信する前記指紋データを暗号化する暗号化手段、および暗号化され受信された前記認証符号を復号化する復号化手段を備えたことを特徴とする請求項1に記載の携帯情報端末。

【請求項3】 前記暗号化には、公開鍵暗号方式を用いることを特徴とする請求項2に記載の携帯情報端末。

【請求項4】 送信する前記指紋データ、および受信する前記認証符号が圧縮コード化されていることを特徴とする請求項1に記載の携帯情報端末。

【請求項5】 前記データ処理装置より受信した認証符号とその有効期限をあわせて表示する表示手段を備えたことを特徴とする請求項1に記載の携帯情報端末。

【請求項6】 前記記憶部に記憶した認証符号を、無効にする手段を備えたことを特徴とする請求項1に記載の携帯情報端末。

【請求項7】 通信機能の操作を行う通信機能操作部を備え、この通信機能操作部の何れかのキー操作に応じて指紋を読み取る手段を設けたことを特徴とする請求項1に記載の携帯情報端末。

【請求項8】 前記通信機能操作部のうち、データ通信開始キーの操作に応じて指紋を読み取る手段を設けたことを特徴とする請求項7に記載の携帯情報端末。

【請求項9】 前記通信機能操作部のうち、通話開始キーの操作に応じて指紋を読み取る手段を設けたことを特徴とする請求項7に記載の携帯情報端末。

【請求項10】 使用者の指紋データをあらかじめ記憶させた第2の記憶部、前記指紋読み取り手段において読み取られた指紋データと前記あらかじめ記憶された指紋データとを照合する照合手段を備え、この照合結果に基づいて、前記指紋データと前記端末識別符号を前記データ処理装置へ送信することを特徴とする請求項1に記載の携帯情報端末。

【請求項11】 携帯情報端末の使用者として登録された者の指紋データと前記携帯情報端末を識別する端末識別符号とを対応させた指紋データ-端末識別符号情報を記憶する記憶部と、この指紋データ-端末識別符号情報

に、前記携帯情報端末から送信された指紋データと端末識別符号を照合する照合手段とを備え、この照合結果に基づいて有効期限を付けた認証符号を発行するデータ処理装置、指紋を読み取る指紋読み取り手段と、この指紋読み取り手段において読み取られた指紋データとあらかじめ記憶された前記端末識別符号とを前記データ処理装置へ送信する送信部と、前記データ処理装置が発行した認証符号を受信する受信部と、前記認証符号と有効期限をあわせて記憶する記憶部とを備えた携帯情報端末、および前記認証符号を受信するサービス端末を含み、サービス端末で受信された認証符号に基づいて携帯情報端末の使用者へ希望するサービスが提供されるサービスシステム。

【請求項12】 前記携帯情報端末と前記データ処理装置との通信の中継を行う交換機を含み、この交換機は、認証符号およびサービス提供依頼が前記サービス端末へ送信される際に、認証符号をあらかじめ定められた対応する音声信号に変換し、この音声信号を前記サービス端末へ送信することを特徴とする請求項11に記載のサービスシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、指紋読み取り手段を備えた携帯情報端末とこれを用いたサービスシステムに関するものである。

【0002】

【従来の技術】例えば、指紋データを用いた本人認証およびサービス提供システムとしては、特開平11-96252号に記載されたものがある。この従来システムは、まずユーザが携帯端末より商品購入指示を出すと、携帯端末で採取した網膜パターンデータおよび指紋データを、あらかじめ口座開設時に網膜パターンデータと指紋データを登録してある銀行へ送信する。次に銀行は送信されたデータと登録してあるデータの照合により本人認証を行い、本人認証にパスすれば、ユーザに対して口座の残高情報を返信する。さらに残高情報を受信したユーザと、このユーザが取引を行った相手は、それぞれ取引結果を前記本人認証を行った銀行へ送信し、これにより銀行において決済が行われるというものである。

【0003】

【発明が解決しようとする課題】以上のような従来システムにおいては、商取引を行う度に決済を行う銀行で本人認証を行う必要があり、商取引時のユーザおよび銀行の作業が煩雑になるという問題点があった。また、ユーザはあらかじめ網膜パターンデータおよび指紋データの登録を、決済に利用するすべての銀行に対し行わなければならない、もしくはあらかじめ登録を行った銀行を利用しなければサービスを受けられず、使い勝手が悪いという問題点があった。

【0004】この発明は上記のような問題点を解決する

ためなされたもので、第1の目的は、一度の本人認証を行うことにより、複数のサービスの提供を受けることができる携帯情報端末を提供することである。

【0005】また、第2の目的は、一度の本人認証を行うことにより、複数のサービスの提供を受けることができるとともに、セキュリティに優れた携帯情報端末を提供することである。

【0006】また、第3の目的は、インターネットを利用して、一度の本人認証を行うことにより、複数のサービスの提供を受けることができるとともに、セキュリティに優れた携帯情報端末を提供することである。

【0007】また、第4の目的は、一度の本人認証を行うことにより、複数のサービスの提供を受けることができるとともに、送受信するデータ量の少ない携帯情報端末を提供することである。

【0008】また、第5の目的は、一度の本人認証を行うことにより、複数のサービスの提供を受けることができるとともに、使い勝手の良い携帯情報端末を提供することである。

【0009】また、第6の目的は、一度の本人認証を行うことにより、複数のサービスの提供を受けることができるとともに、本人以外が不正にサービスの提供を受けることを防止できる携帯情報端末を提供することである。

【0010】また、第7の目的は、一度の本人認証を行うことにより、複数のサービスの提供を受けることができるとともに、利用者の制限が可能な携帯情報端末を提供することである。

【0011】また、第8の目的は、一度の本人認証を行うことにより、複数のサービスの提供を受けることができるサービスシステムを提供することである。

【0012】また、第9の目的は、一度の本人認証を行うことにより、複数のサービスの提供を受けることができるとともに、サービス端末の使い勝手が良いサービスシステムを提供することである。

【0013】

【課題を解決するための手段】この発明に係る携帯情報端末は、携帯情報端末の利用者として登録された者の指紋データと携帯情報端末を識別する端末識別符号とを対応させた指紋データ-端末識別符号情報に、携帯情報端末から送信された指紋データと端末識別符号を照合し、この照合結果に基づき有効期限を付けた認証符号を発行するデータ処理装置と通信を行うものであって、指紋を読み取り指紋データを生成する指紋読み取り手段、指紋データとあらかじめ記憶された端末識別符号をデータ処理装置へ送信する送信部、認証符号を受信する受信部、および受信した認証符号と有効期限を記憶する記憶部を備えるようにしたものである。

【0014】また、この発明に係る携帯情報端末は、前記指紋読み取り手段、前記送信部、前記受信部、前記記

憶部に加え、送信する指紋データを暗号化する暗号化手段、および暗号化され受信された認証符号を復号化する復号化手段を備えるようにしたものである。

【0015】また、この発明に係る携帯情報端末は、前記指紋読み取り手段、前記送信部、前記受信部、前記記憶部に加え、送信する指紋データを暗号化する暗号化手段、および暗号化され受信された認証符号を復号化する復号化手段を備え、暗号化には公開鍵暗号方式を用いるようにしたものである。

【0016】また、この発明に係る携帯情報端末は、前記指紋読み取り手段、前記送信部、前記受信部、前記記憶部を備え、送信する指紋データおよび受信する認証符号を圧縮コード化するようにしたものである。

【0017】また、この発明に係る携帯情報端末は、前記指紋読み取り手段、前記送信部、前記受信部、前記記憶部に加え、受信した認証符号とその有効期限を表示する表示手段を備えるようにしたものである。

【0018】また、この発明に係る携帯情報端末は、前記指紋読み取り手段、前記送信部、前記受信部、前記記憶部に加え、記憶部に記憶した認証符号を、無効にする手段を備えるようにしたものである。

【0019】また、この発明に係る携帯情報端末は、前記指紋読み取り手段、前記送信部、前記受信部、前記記憶部に加え、通信機能の操作を行う通信機能操作部を備え、通信機能操作部の何れかのキー操作に応じて指紋を読み取る手段を設けるようにしたものである。

【0020】また、この発明に係る携帯情報端末は、前記指紋読み取り手段、前記送信部、前記受信部、前記記憶部に加え、通信機能の操作を行う通信機能操作部を備え、通信機能操作部のうち、データ通信開始キーの操作に応じて指紋を読み取る手段を設けるようにしたものである。

【0021】また、この発明に係る携帯情報端末は、前記指紋読み取り手段、前記送信部、前記受信部、前記記憶部に加え、通信機能の操作を行う通信機能操作部を備え、通信機能操作部のうち、通話開始キーの操作に応じて指紋を読み取る手段を設けるようにしたものである。

【0022】また、この発明に係る携帯情報端末は、前記指紋読み取り手段、前記送信部、前記受信部、前記記憶部に加え、使用者の指紋データをあらかじめ記憶している第2の記憶部、および読み取られた指紋データと記憶している指紋データとを照合する照合手段を備え、照合結果に基づいて、指紋データと端末識別符号をデータ処理装置へ送信するようにしたものである。

【0023】また、この発明に係るサービスシステムは、携帯情報端末の利用者として登録された者の指紋データと携帯情報端末を識別する端末識別符号とを対応させた指紋データ-端末識別符号情報を記憶する記憶部と、指紋データ-端末識別符号情報に、携帯情報端末から送信された指紋データと端末識別符号を照合する照合

手段とを備え、照合結果に基づいて有効期限を付けた認証符号を発行するデータ処理装置、指紋を読み取る指紋読み取り手段と、読み取られた指紋データとあらかじめ記憶された端末識別符号をデータ処理装置へ送信する送信部と、認証符号を受信する受信部と、受信した認証符号と有効期限を記憶する記憶部とを備えた携帯情報端末、および認証符号を受信するサービス端末を含み、サービス端末で受信された認証符号に基づいて携帯情報端末の使用者へ希望するサービスが提供されるようにしたものである。

【0024】また、この発明に係るサービスシステムは、前記データ処理装置と、前記携帯情報端末と、前記サービス端末に加え、携帯情報端末とデータ処理装置との通信の中継を行う交換機を含み、交換機が認証符号およびサービス提供依頼がサービス端末へ送信される際に、認証符号をあらかじめ定められた対応する音声信号に変換し、この音声信号をサービス端末へ送信するようにしたものである。

【0025】

【発明の実施の形態】実施の形態1. 図1は、この発明の実施の形態1における携帯情報端末の外観概略図である。この携帯情報端末はデータ通信用携帯端末であり、直方体形状の筐体1を有し、この筐体1の主面1aには、電話番号、文字などの入力、データ通信の開始、および通話などの通信機能の操作を行う通信機能操作部3と、液晶ディスプレイ2が設けられている。この通信機能操作部3に含まれるデータ通信開始キー3aは、その内側から透過して画像認識を行い指紋を読みとれるように透明な樹脂で構成されており、指紋を読み取るために十分な大きさを持つ。データ通信開始キー3aの内側には、そのキーの表面に接触した指の指紋を画像認識により読み取り、指紋データを生成する指紋読み取り装置が設けられている。データ通信開始キー3aは、その押下によって、指紋読み取り装置を動作させるとともに、生成された指紋データに基づいてデータ通信の開始を指示する機能を持つ。また液晶ディスプレイ2は、通信機能操作部3によって入力される相手局電話番号表示、発信または着信メール表示などを行うとともに、後で説明する認証符号およびその有効期限を表示する表示手段である。

【0026】図2は、実施の形態1の携帯情報端末の内部回路を示すブロック図である。通信機能操作部3の一つのキーであるデータ通信開始キー3aは、そのキー操作に応じて指紋を読み取る手段である指紋読み取り装置41と接続しており、データ通信開始キー3aを押下することにより、指紋読み取り装置41が動作し、使用者（ユーザ）の指紋を読み取る。指紋読み取り装置41にて読み取られた指紋データは、制御部36に送られる。制御部36は、CPU37、あらかじめ登録された端末識別符号（端末ID）と使用者の指紋データを記憶して

いる第1の記憶部38、後で説明する認証符号（認証ID）とその有効期限を記憶する第2の記憶部39、および照合手段40から構成されており、第1、第2の記憶部38、39、および照合手段40はCPU37に接続されている。照合手段40において制御部36に送られた指紋データと第1の記憶部に記憶された指紋データの照合が行われる。CPU37は、この照合手段40で一致が確認されると、本人認証を行うためのデータ通信を開始する制御を行う。

10 【0027】本人認証を行うためのデータ通信が開始されると、指紋データは第1の記憶部38から読み出された端末識別符号とともに暗号化手段34において公開鍵暗号方式を用いて暗号化され、送信部32によりアンテナ31を介し送信される。ここで送信される指紋データは、一致が確認されているので、データ通信開始キー3aが押下されたときに指紋読み取り装置41によって読み取られたものでも、第1の記憶部38にあらかじめ記憶されたものでもどちらでもよい。

【0028】受信部33は、後で説明するデータ処理装置で発行された認証符号とその有効期限をアンテナ31より受信する。この認証符号および有効期限は公開鍵暗号方式を用いて暗号化されており、認証符号、有効期限とともに復号化手段35によって復号化され、第2の記憶部39に記憶されると同時に、液晶ディスプレイ2に表示される。また、この認証符号とその有効期限は、適宜、液晶ディスプレイ2に表示することが可能である。これにより、ユーザは認証符号の有効期限を必要に応じて確認することができ、有効期限の切れた認証符号を誤って使用することを防止する効果が得られる。

30 【0029】また、この認証符号は、ユーザによって無効にすることが可能である。CPU37は、記憶部38より端末識別符号を、記憶部39より認証符号を読み出し、これらを暗号化手段34において公開鍵暗号方式を用いて暗号化し、送信部32により送信する制御を行う。後で説明するデータ処理装置は、端末識別符号と認証符号をあわせて受信すると、この認証符号を有効期限内であっても無効にする。これにより、携帯情報端末の盗難などにより、本人以外が認証符号を不正使用することを防止する効果が得られる。また、ユーザが認証符号を無効にすることを忘れる、あるいは回線トラブルなどで上記手続きによる無効ができなかった場合でも、あらかじめ適切な値に設定された有効期限により、本人以外が認証符号を不正使用することを防止できる。

40 【0030】図3は実施の形態1におけるサービスシステムの構成図である。図に示すようにこのサービスシステムは、上記で説明した構成の携帯情報端末12、データ処理装置4、およびサービス端末9を含んで構成されており、それぞれはインターネット網8に接続可能である。データ処理装置4は、公的機関などに設けられるもので、あらかじめ使用者として登録された携帯情報端末

のユーザの指紋データと、その携帯情報端末を識別する端末識別符号とを対応させた指紋データ-端末識別符号情報(指紋DB)7を記憶した記憶部6、およびこれに接続されたコンピュータ5を備えており、コンピュータ5は、携帯情報端末12から送信された端末識別符号に基づいて記憶部6より対応する指紋データを読み出し、この指紋データと携帯情報端末12から送信された指紋データとを照合する照合機能を持つ。サービス端末9は、たとえばユーザに対しデータを提供するデータ提供者、または商品を提供する商品販売業者などに設置されているものであって、ユーザから送信されたサービス依頼内容、認証符号などを一時的に記憶する記憶部11、およびこれに接続されデータの入出力制御を行うコンピュータ10を備えている。

【0031】図4は、データ処理装置4に記憶された指紋データ-端末識別符号情報7のデータフォーマットを示している。端末識別符号13および指紋データ14はあらかじめ対応して登録されており、携帯情報端末12から送信された指紋データと端末識別符号を照合の結果、本人認証がなされると、有効期限16が設定された認証符号15が発行され、同時に認証符号15およびその有効期限16が指紋データ-端末識別符号情報7に書き込まれる。

【0032】次にこの実施の形態1の携帯情報端末およびこれを用いたサービスシステムの動作について、図5に示すフローチャートを用いて説明する。まず、携帯情報端末12において、ユーザがデータ通信開始キー3aを押下することにより、指紋読み取り装置41が動作し指紋データの採取が行われる(ステップS51)。採取された指紋データは、制御部36に送られ、照合手段40において、CPU37が第1の記憶部38から読み出した指紋データと照合される(ステップS52)。

【0033】ステップS53において、一致が確認されユーザがこの携帯情報端末12の使用者であることが認証(本人認証)されると、データ通信が開始される。本人認証がされない場合は、本人認証に失敗したことが液晶ディスプレイ2に表示される(ステップS54)。データ通信が開始されると、CPU37によって第1の記憶部38から読み出された端末識別符号は指紋データとともに暗号化手段34で公開鍵暗号方式を用いて暗号化され、送信部32によりデータ処理装置4へ送信される(ステップS55)。

【0034】本人認証がされその結果に基づいてデータ通信が開始されるので、この携帯情報端末12の登録された使用者以外がデータ処理装置4に対し端末識別符号および指紋データを送信することを防止できる。さらに、データ処理装置4が登録された使用者以外のデータを処理することを防止でき、不要な通信および処理を削減する効果が得られる。

【0035】携帯情報端末12が送信した端末識別符号

と指紋データを受信したデータ処理装置4は、それらの復号化を行い、コンピュータ5が受信した指紋データと端末識別符号を記憶部6に記憶された指紋データ-端末識別符号情報7に照合する(ステップS56)。ステップS57において、コンピュータ5が一致を確認し、送信したユーザが携帯情報端末12の登録された使用者であることを認証(本人認証)すると、有効期限が設定された認証符号が発行され、公開鍵暗号方式で暗号化されて携帯情報端末12へ送信される。同時に認証符号およびその有効期限は、指紋データ-端末識別符号情報7に書き込まれ、コンピュータ5はタイマを張って、有効期限の管理を行う(ステップS58)。

【0036】ステップS56において、本人認証がされない場合、データ処理装置4は、携帯情報端末12へ本人認証が失敗したことを通知する(ステップS59)。通知を受信した携帯情報端末12は、本人認証が失敗したことを液晶ディスプレイ2に表示する(ステップS54)。

【0037】携帯情報端末12は、データ処理装置4が発行し送信した認証符号を受信部33で受信し復号化手段35で復号化を行い、第2の記憶部に認証符号とその有効期限をあわせて記憶する(ステップS60)。なお、記憶された認証符号とその有効期限は、液晶ディスプレイ2に表示が可能であり、ステップS60において記憶部に記憶されると同時に表示されるとともに、認証符号を使用時に再度表示することが可能である。

【0038】携帯情報端末12のユーザは、サービス提供を依頼する場合、記憶した認証符号と依頼するサービス内容を暗号化手段34にて公開鍵暗号方式を用いて暗号化し、送信部32よりサービス端末9へ送信する(ステップS61)。

【0039】携帯情報端末12が送信した認証符号とサービス内容を受信したサービス端末9は、受信した認証符号をデータ処理装置4へ送り、認証符号の確認を依頼する(ステップS62)。データ処理装置4は、受信した認証符号に対応する指紋データ-端末識別符号情報7に書き込まれた有効期限を確認し(ステップS63)、有効期限内であれば認証符号を確認した旨をサービス端末9へ返信する(ステップS64)。受信した認証符号に対応する指紋データ-端末識別符号情報がない、または有効期限が切れている場合は、認証符号が確認できなかった旨をサービス端末9へ返信する(ステップS65)。

【0040】サービス端末9が認証符号を確認した旨の通知を得た場合は、携帯情報端末12から依頼されたサービス内容が実施される(ステップS66)。サービス端末9が認証符号を確認できなかった旨の通知を得た場合は、携帯情報端末12に対し、依頼されたサービスを拒否する通知が行われる(ステップS67)。

【0041】以上のように、データ処理装置4におい

て、有効期限の定められた認証符号が発行され、携帯情報端末12において、この認証符号をその有効期限とともに記憶するようにしたので、一度の本人認証手続きを行うことにより、有効期限内であれば何度でも認証符号を用いたサービス提供を依頼することが可能となる。

【0042】また、携帯情報端末12において、データ通信開始キー3aの押下によって指紋読み取り装置41が動作し、指紋が読み取られるようにしたので、使用者の使い勝手がよい。

【0043】また、このサービスシステムにおいて通信される端末識別符号、指紋データ、認証符号およびサービス内容について、暗号化を行うようにしたので、セキュリティの高い本人認証手続きが可能となる。

【0044】さらに、暗号化には公開鍵暗号方式を用いたので、データ処理装置4をインターネット上に設けることができる。

【0045】なお、このサービスシステムにおいて通信される端末識別符号、指紋データ、認証符号およびサービス内容について、圧縮コード化を行っても良い。この場合、通信データ量を削減できるという効果が得られる。また、携帯情報端末は、通信機能を持つパソコンなどであっても良く、その場合も同様の効果が得られる。

【0046】実施の形態2。図6はこの発明の実施の形態2である携帯情報端末の外観概略図である。図において、図1と同じ番号が付されたものは同じものを示すため説明を省略する。この携帯情報端末は、音声通話ができる電話機能を持つ携帯電話であり、通話相手の音声を出力するスピーカ17とユーザの音声を入力するマイクロホン18を備えている。3bは通信機能操作部3に含まれる通話開始キーであり、その内側から透過して画像認識を行い指紋を読みとれるように透明な樹脂で構成されており、指紋を読み取るために十分な大きさを持つ。通話開始キー3bの内側には、そのキーの表面に接触した指の指紋を画像認識により読み取り、指紋データを生成する指紋読み取り装置が設けられている。通話開始キー3bは、その押下によって、指紋読み取り装置を動作させるとともに、生成された指紋データに基づいて通話接続の開始を指示する機能を持つ。

【0047】図7は、実施の形態2の携帯情報端末の内部回路を示すブロック図である。図において、図2と同じ番号が付されたものは同じものを示すため説明を省略する。3bは、通信機能操作部3の一つのキーであり、押下することにより、指紋読み取り装置41が動作し、ユーザの指紋を読み取る。実施の形態1と同様にして読み取られた指紋データの一致が確認されると、本人認証を行うための通話接続手順が開始される。

【0048】本人認証を行うための通話接続手順が開始されると、指紋データは端末識別符号とともに暗号化手段34において後で説明する交換機とあらかじめ定められた暗号方式を用いて暗号化される。また、受信した認

証符号は上記の暗号方式を用いて暗号化されており、復号化手段35によって復号化される。

【0049】また、レシーバ17、マイクロホン18は、制御部36に含まれCPU37に接続されたD/A変換器42、A/D変換器43にそれぞれ接続され、通話時に音声信号の入出力を行う。

【0050】図8は実施の形態2におけるサービスシステムの構成図である。図に示すようにこのサービスシステムは、上記で説明した構成の携帯情報端末12、実施の形態1で説明したデータ処理装置4に加えて、基地局などに設けられたものであって携帯情報端末12とデータ処理装置4の通信の中継を行う交換機19、および音声通話用電話であるサービス端末23を含んで構成されており、データ処理装置4と交換機19はインターネット網8に接続されている。交換機19は、携帯情報端末12およびデータ処理装置4から受信する信号を所定の暗号方式で復号化する復号化手段21と、携帯情報端末12およびデータ処理装置4へ送信する信号を所定の暗号方式で暗号化する暗号化手段20と、これらに接続され、認証結果に基づき認証符号をあらかじめ定められた対応する音声信号に変換する音声変換器22とを備えている。サービス端末23は、たとえばユーザに対し商品を提供する商品販売業者などに設置されているものであって、ユーザからのサービス依頼および本人認証結果を音声信号で受信する音声通話用電話である。

【0051】次にこの実施の形態2の携帯情報端末およびこれを用いたサービスシステムの動作について、図9に示すフローチャートを用いて説明する。まず、携帯情報端末12において、ユーザが本人認証を必要とするサービス依頼を行うためにサービス提供者の電話番号を入力し通話開始キー3bを押下し、これにより指紋読み取り装置41が動作して指紋データの採取が行われる(ステップS71)。採取された指紋データは、制御部36に送られ、照合手段40において、CPU37が第1の記憶部38から読み出した指紋データと照合される(ステップS72)。

【0052】ステップS73において、一致が確認されユーザがこの携帯情報端末12の使用者であることが認証(本人認証)されると、通話接続手順が開始される。本人認証がされない場合は、本人認証に失敗したことが液晶ディスプレイ2に表示される(ステップS74)。通話接続手順が開始されると、CPU37によって第1の記憶部38から読み出された端末識別符号は指紋データとともに暗号化手段34において、交換機19との間であらかじめ定められた暗号方式で暗号化され、送信部32により交換機19へ送信される(ステップS75)。

【0053】交換機19は、受信した指紋データと端末識別符号を復号化手段21で一旦復号化し、さらに暗号化手段20で公開鍵暗号方式を用いて暗号化して、イン

ターネット上のデータ処理装置4へ送信する(ステップS76)。データ処理装置4は、受信した指紋データと端末識別符号の復号化を行い、コンピュータ5がそれらを記憶部6に記憶された指紋データ-端末識別符号情報7に照合する(ステップS77)。ステップS78において、コンピュータ5が一致を確認し、送信したユーザを本人認証すると、有効期限が設定された認証符号が発行され、公開鍵暗号方式で暗号化されて交換機19へ送信される。同時に認証符号およびその有効期限は、指紋データ-端末識別符号情報7に書き込まれ、コンピュータ5はタイマを張って、有効期限の管理を行う(ステップS79)。

【0054】ステップS78において、本人認証がされない場合、データ処理装置4は、交換機19を経由して携帯情報端末12へ本人認証が失敗したことを通知する(ステップS80)。通知を受信した携帯情報端末12は、本人認証が失敗したことを液晶ディスプレイ2に表示する(ステップS74)。

【0055】認証符号を受信した交換機19は、それを復号化手段21で一旦復号化し、さらに暗号化手段20で携帯情報端末12との間であらかじめ定められた暗号方式を用いて暗号化して携帯情報端末12へ送信するとともに、ユーザがサービス依頼を行う相手であるサービス端末23へ通話を接続する処理を行い、サービス端末23へサービス依頼主が本人認証された旨を音声信号で通知する(ステップS81)。

【0056】このとき通知する音声信号は、音声変換器22で生成されたものであって、たとえば「サービス依頼主は認証符号××××号によって本人認証された端末識別符号×××××の携帯情報端末の使用者です」などとする。サービス端末23が本人認証された旨の通知を受け、通話によってサービスが依頼されると、サービス内容が実施される(ステップS96)。

【0057】交換機19から認証符号を受信した携帯情報端末12は、復号化を行い、第2の記憶部に認証符号とその有効期限をあわせて記憶する(ステップS82)と同時に、液晶ディスプレイ2に表示する。

【0058】有効期限内に別のサービス提供依頼に対し上記の説明で取得した認証符号を使用する場合は、携帯情報端末12は認証符号を暗号化して交換機19に送付する(ステップS91)。交換機19は受信した認証符号をデータ処理装置4に送り、認証符号の確認を行う(ステップS92)。ステップS93において、認証符号が有効期限内であることを確認されると、交換機19は、ユーザがサービス依頼を行う相手であるサービス端末23と携帯情報端末12の通話を接続する処理を行い、サービス端末23へサービス依頼主が本人認証された旨を音声信号で通知する(ステップS94)。サービス端末23が本人認証された旨の通知を受け、通話によってサービスが依頼されると、サービス内容が実施され

る(ステップS96)。

【0059】ステップS93において、認証符号が有効期限内であることが確認されなかった場合、交換機19は、認証されなかった旨を携帯情報端末12へ通知し(ステップS95)、通知を受信した携帯情報端末12は、本人認証が失敗したことを液晶ディスプレイ2に表示する(ステップS74)。

【0060】以上のように、データ処理装置4において、有効期限の定められた認証符号が発行され、携帯情報端末12において、この認証符号をその有効期限とともに記憶するようにしたので、一度の本人認証手続きを行うことにより、有効期限内であれば何度でも認証符号を用いたサービス提供を依頼することが可能となる。

【0061】また、携帯情報端末12において、通話開始キー3bの押下によって指紋読み取り装置41が動作し、指紋が読み取られるようにしたので、使用者の使い勝手がよい。

【0062】また、このサービスシステムにおいて通信される端末識別符号、指紋データ、認証符号およびサービス内容について、暗号化を行うようにしたので、セキュリティの高い本人認証手続きが可能となる。

【0063】さらに、このサービスシステムに交換機を含み、交換機が、本人認証の確認された旨を音声信号にてサービス端末へ通知するようにしたので、サービス端末はデータ通信機能のない電話機でもよく、使い勝手が良い。

【0064】

【発明の効果】以上のようにこの発明によれば、データ処理装置において、有効期限の定められた認証符号を発行し、携帯情報端末において、この認証符号をその有効期限とともに記憶するようにしたので、一度の本人認証を行うことにより、複数のサービス提供を受けることができる。

【0065】また、この発明によれば、指紋データおよび認証符号を暗号化して送信するようにしたので、セキュリティに優れた携帯情報端末を提供できる。

【0066】また、この発明によれば、指紋データおよび認証符号の暗号化を公開鍵暗号方式を用いて行うようにしたので、データ処理装置をインターネット上に設けることができる。

【0067】また、この発明によれば、指紋データおよび認証符号を圧縮コード化して送信するようにしたので、送受信するデータ量の少ない携帯情報端末を提供できる。

【0068】また、この発明によれば、携帯情報端末において、取得した認証符号とその有効期限を表示するようにしたので、有効期限の確認が容易にでき、使い勝手がよい。

【0069】また、この発明によれば、携帯情報端末において、記憶部に記憶した認証番号を無効にするように

したので、本人以外が不正にサービスの提供を受けることを防止できる。

【0070】また、この発明によれば、携帯情報端末のデータ通信開始キーまたは通話開始キーに指紋読み取り手段を設けたので、通信の開始動作によって指紋データの採取が行われ、使い勝手がよい。

【0071】また、この発明によれば、携帯情報端末において指紋データの照合を行い、本人認証後に端末識別符号および指紋データを送信するようにしたので、利用者の制限ができる。

【0072】また、この発明によれば、サービスシステムに交換機を含み、交換機が、認証符号を対応する音声信号に変換してサービス端末へ通知するようにしたので、サービス端末はデータ通信機能のない電話機でもよく、使い勝手が良いサービスシステムを提供できる。

【図面の簡単な説明】

【図1】 本発明の実施の形態1における携帯情報端末の外観概略図である。

【図2】 本発明の実施の形態1における携帯情報端末の内部回路を示すブロック図である。

【図3】 本発明の実施の形態1におけるサービスシステムの構成図である。

【図4】 本発明の実施の形態1における指紋データ端末識別符号情報のデータフォーマット図である。

【図5】 本発明の実施の形態1における携帯情報端末およびサービスシステムの動作を示すフローチャートである。

【図6】 本発明の実施の形態2における携帯情報端末の外観概略図である。

【図7】 本発明の実施の形態2における携帯情報端末の内部回路を示すブロック図である。

【図8】 本発明の実施の形態2におけるサービスシステムの構成図である。

【図9】 本発明の実施の形態2における携帯情報端末およびサービスシステムの動作を示すフローチャートである。

【符号の説明】

2 液晶ディスプレイ（表示手段）

3 通信機能操作部

3a データ通信開始キー

10 3b 通話開始キー

4 データ処理装置

5 コンピュータ（照合手段）

6 記憶部

7 指紋データ・端末識別符号情報

9 サービス端末

12 携帯情報端末

13 端末識別符号

14 指紋データ

15 認証符号

20 16 認証符号有効期限

19 交換機

23 サービス端末

32 送信部

33 受信部

34 暗号化手段

35 復号化手段

37 CPU

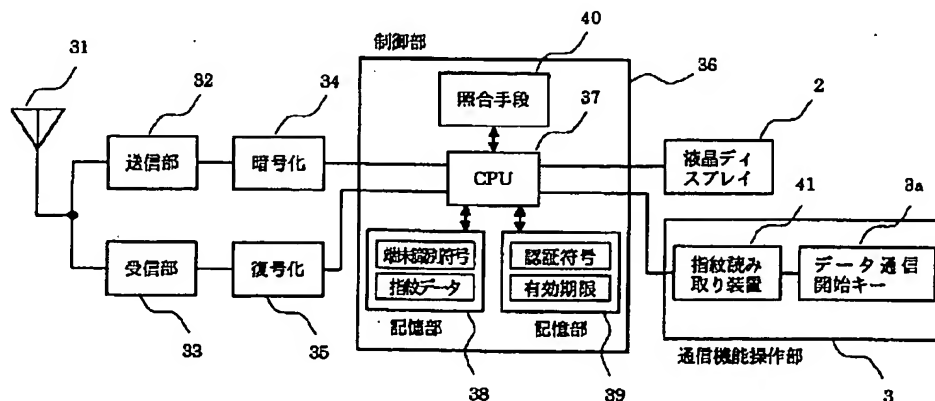
38 記憶部

39 記憶部

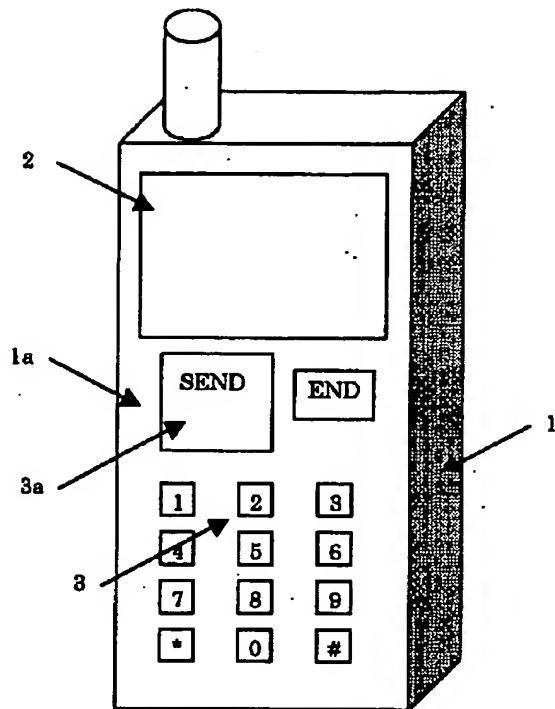
30 40 照合手段

41 指紋読み取り装置（指紋読み取り手段）

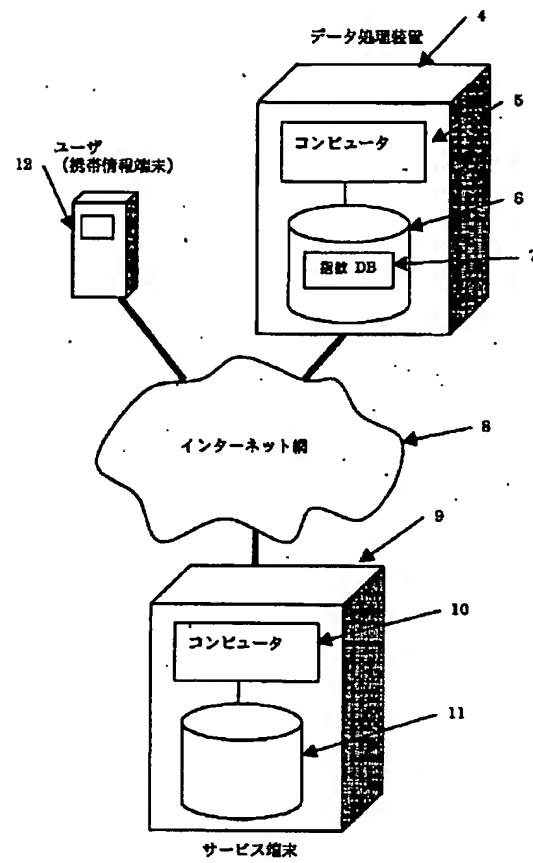
【図2】



【図1】



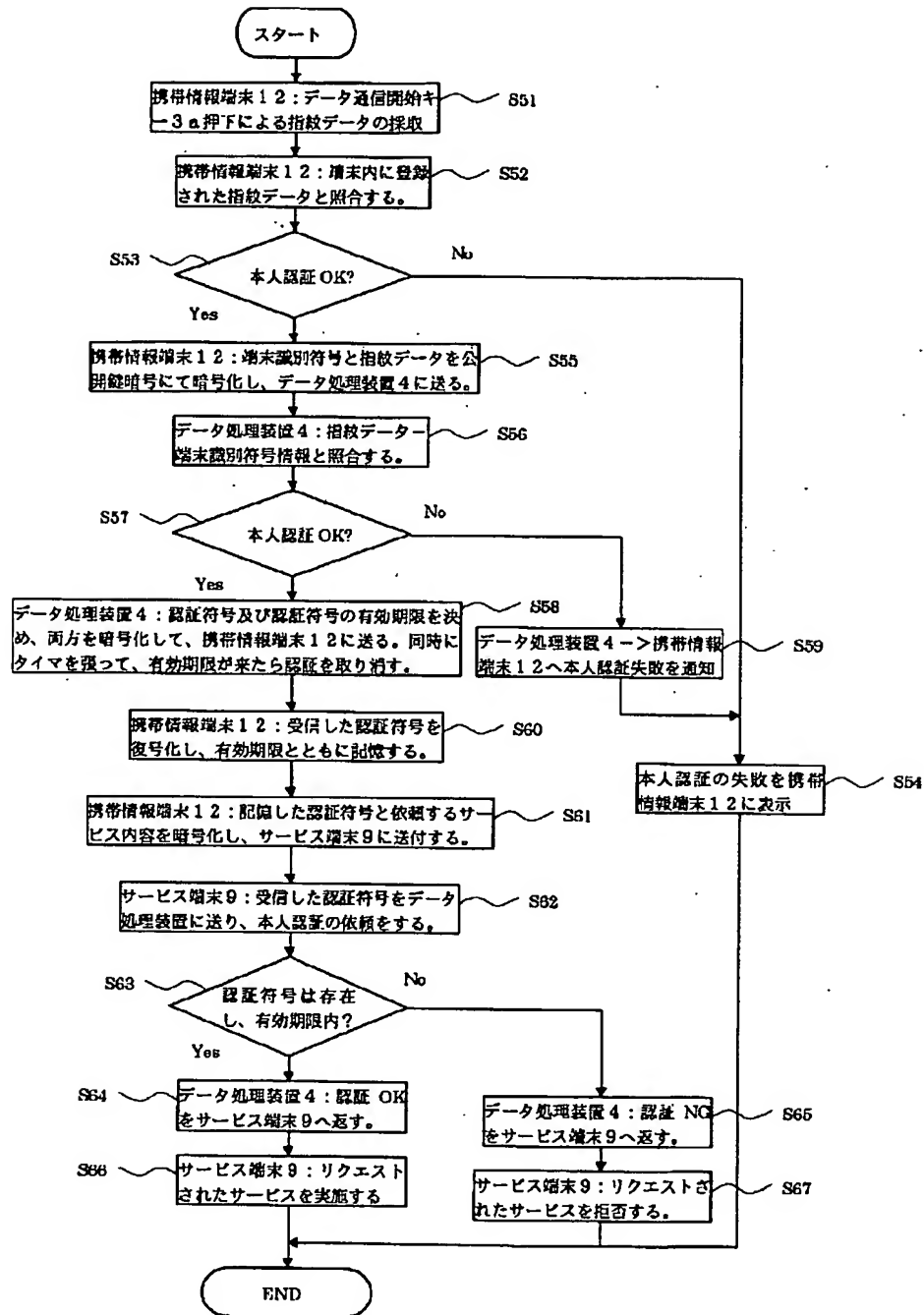
【図3】



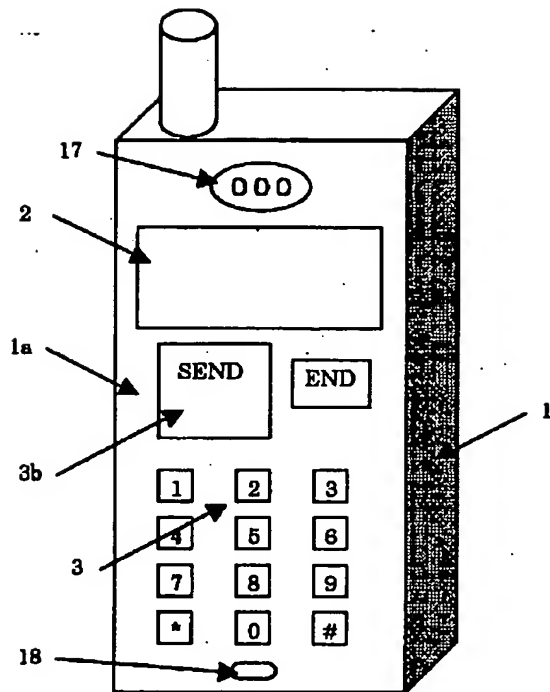
【図4】

端末識別符号	指紋データ	認証符号	認証符号有効期限
1234567890	User 指紋 Data	00000001	00/02/25 15:15:30
1234567891	User 指紋 Data	0	—
:	:	:	:

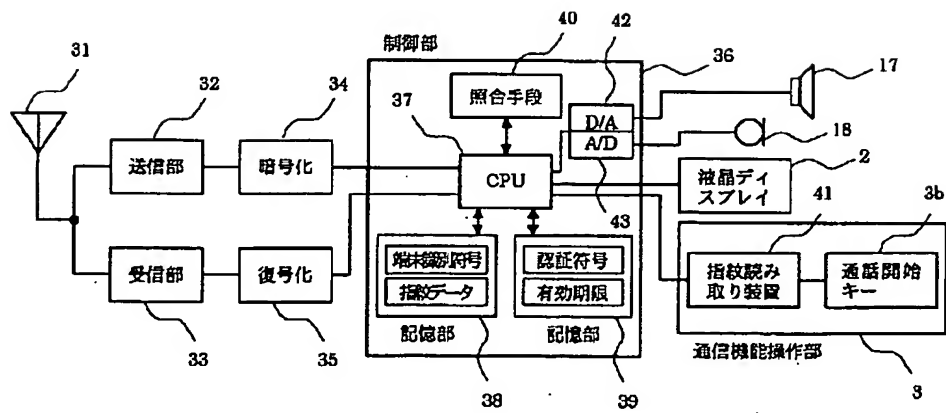
【図5】



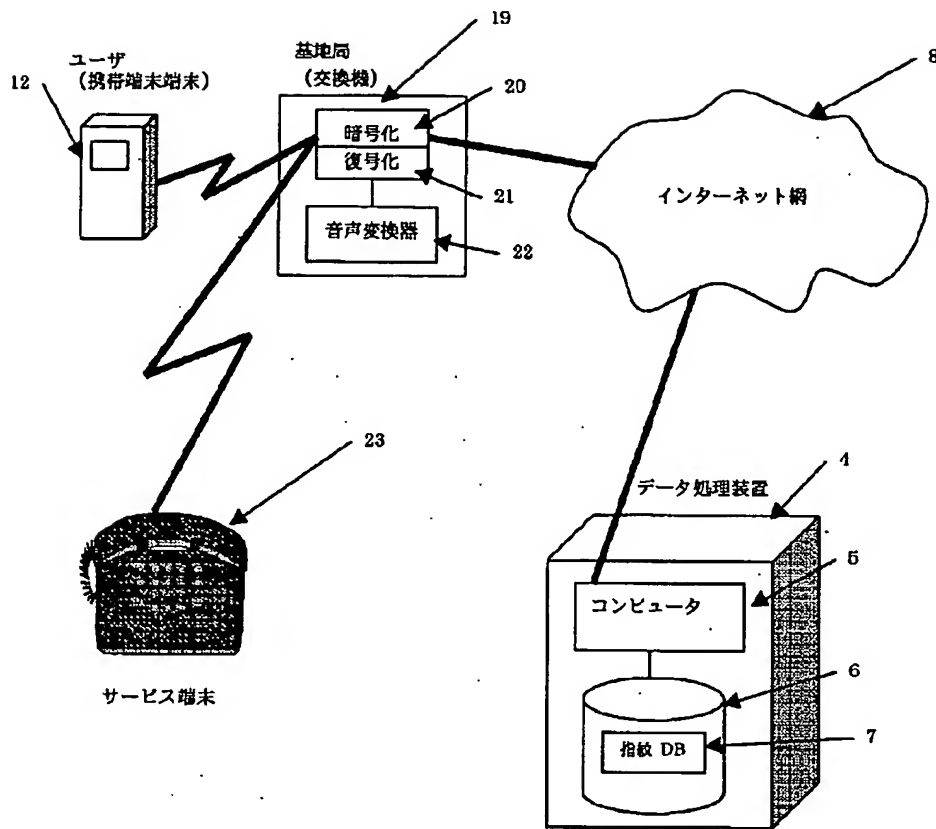
【図6】



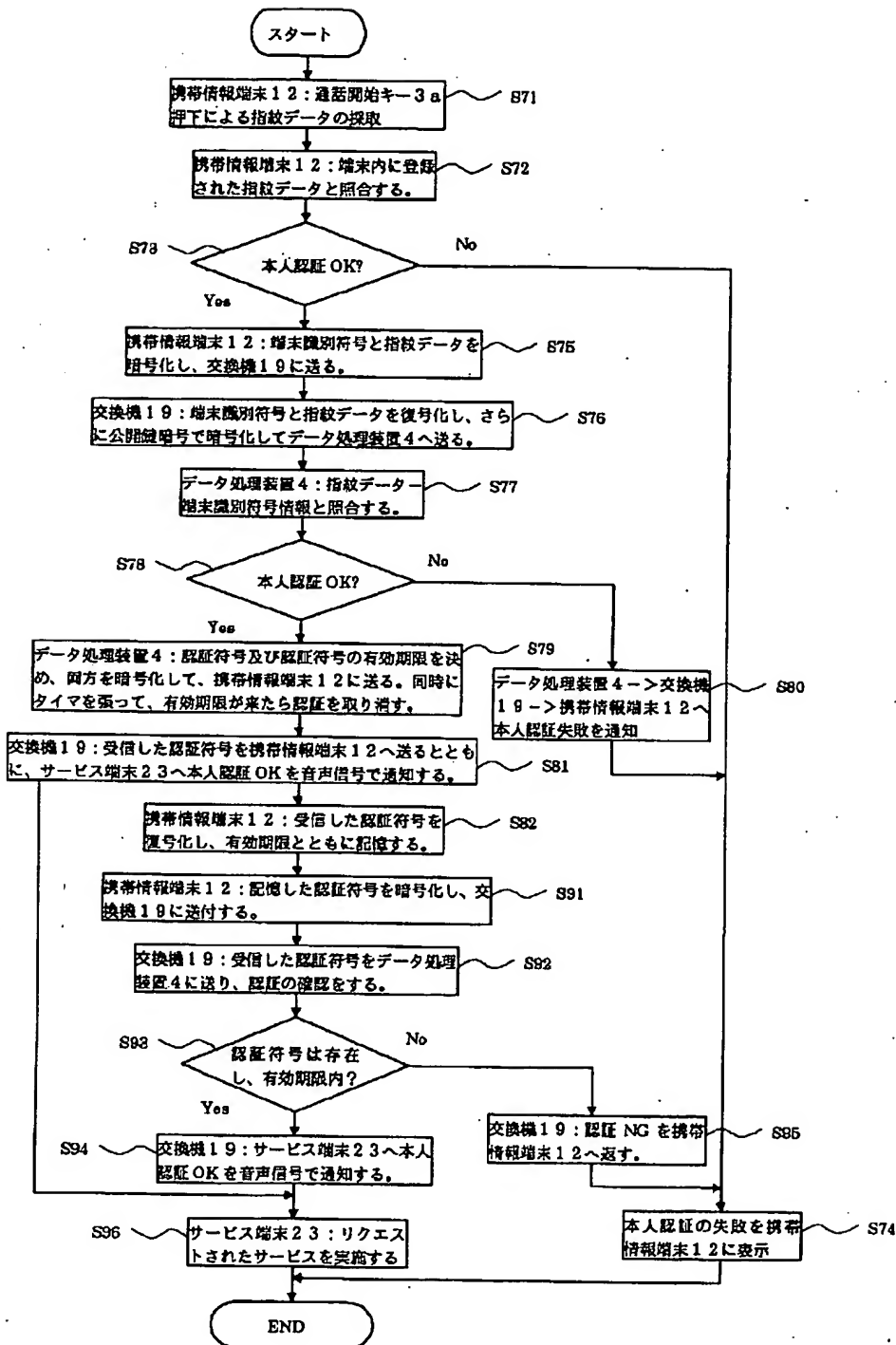
【図7】



【図8】



【図9】



フロントページの続き

(51)Int.Cl. ⁷	識別記号	F I	ターム(参考)
H 0 4 M 3/42		H 0 4 B 7/26	1 0 9 R 5 K 1 0 1
11/00	3 0 2	H 0 4 L 9/00	6 7 3 D 9 A 0 0 1
			6 7 3 A

Fターム(参考) 5J104 AA07 KA01 KA17 PA02 PA10
5K024 AA62 AA76 CC11 DD01 DD02
DD04 FF05 GG01 GG05
5K027 AA11 BB09 HH23
5K051 CC01 JJ07 JJ13 JJ16 JJ17
5K067 AA33 BB00 BB04 BB21 EE02
EE16 GG01 GG11 HH05 HH22
HH23 HH24
5K101 LL12 NN06 PP04
9A001 EE03 EE04 EE05 JJ25 LL03